RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: MASH-M05

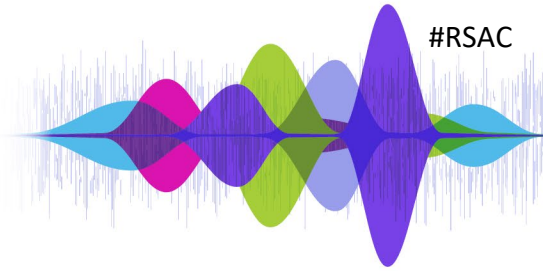
Cybersecurity Myth-Busting: Fact vs. Fiction in Cyber Programs

Daniel Gorecki

CISO
NGC Risk
https://www.linkedin.com/in/dangorecki/

Scott Brammer

CISO @ RegEd
Podcast Host @ The Cyber Security Council
https://www.linkedin.com/in/scott-brammer/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The views and opinions expressed in this program are those of the speakers and do not necessarily reflect the views or positions of any entities they represent.

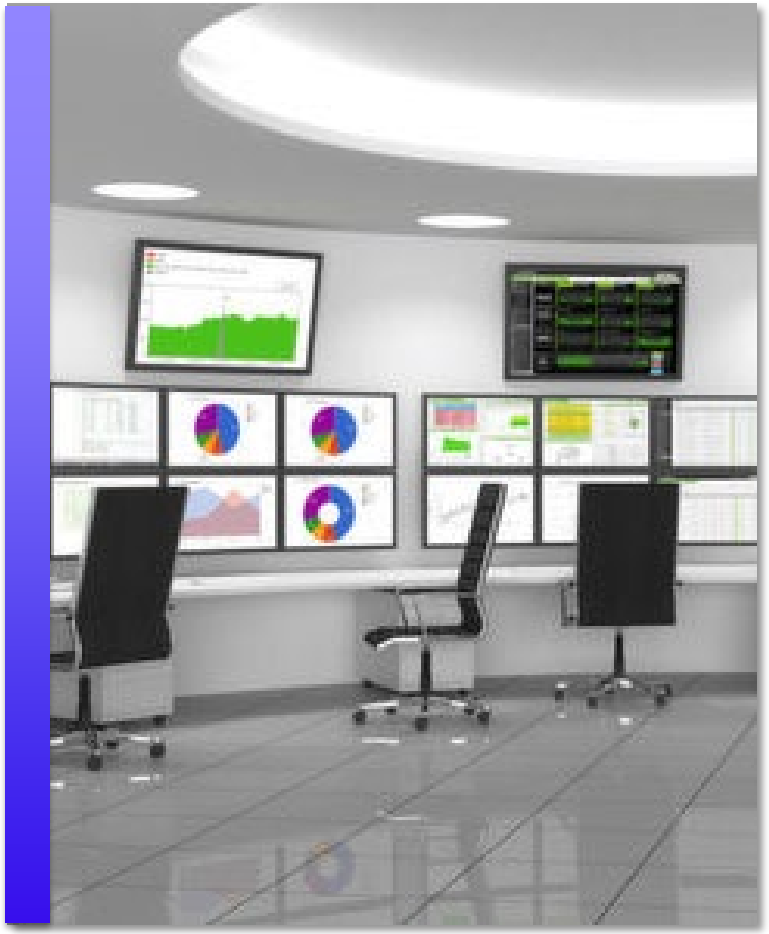
What is a myth?

- Merriam Webster: Myth: noun
  - a usually traditional story of ostensibly historical events that serves to unfold part of the world view of a people or explain a practice, belief, or natural phenomenon
  - a popular belief or tradition that has grown up around something or someone
    - *especially*: one embodying the ideals and institutions of a society or segment of society

Ready for a game?

- We present a Cyber Myth
- We'll confront the Myth with 🔍 **Analysis**
- We'll give a ⚖️ **Verdict** on the Myth:
  - ✅ CONFIRMED
  - ⚠️ PLAUSIBLE
  - 🚨 BUSTED
- We'll provide a 🛠️ **Takeaway**

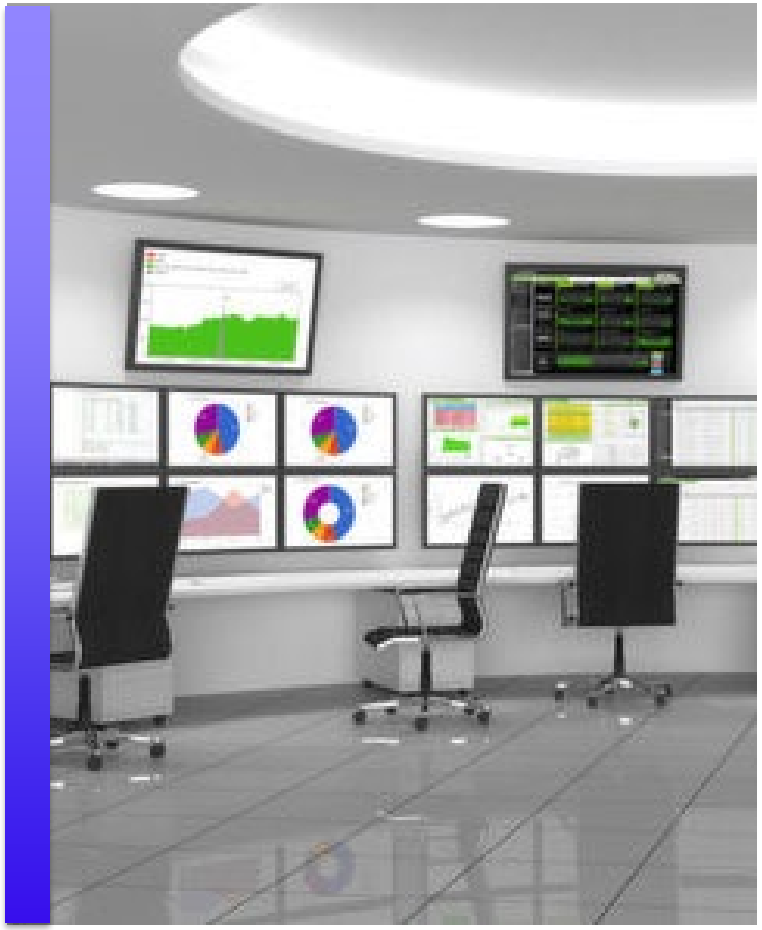
Myth 1: Your Security Operations Center (SOC) is part of your 1st line of defense.



Myth 1: Your Security Operations Center (SOC) is part of your 1st line of defense.

🔍 **Analysis:**

- The "True" First Line
- Operational ≠ First Line; Detection ≠ Prevention
- Assurance Role



Myth 1: Your Security Operations Center (SOC) is part of your 1st line of defense.

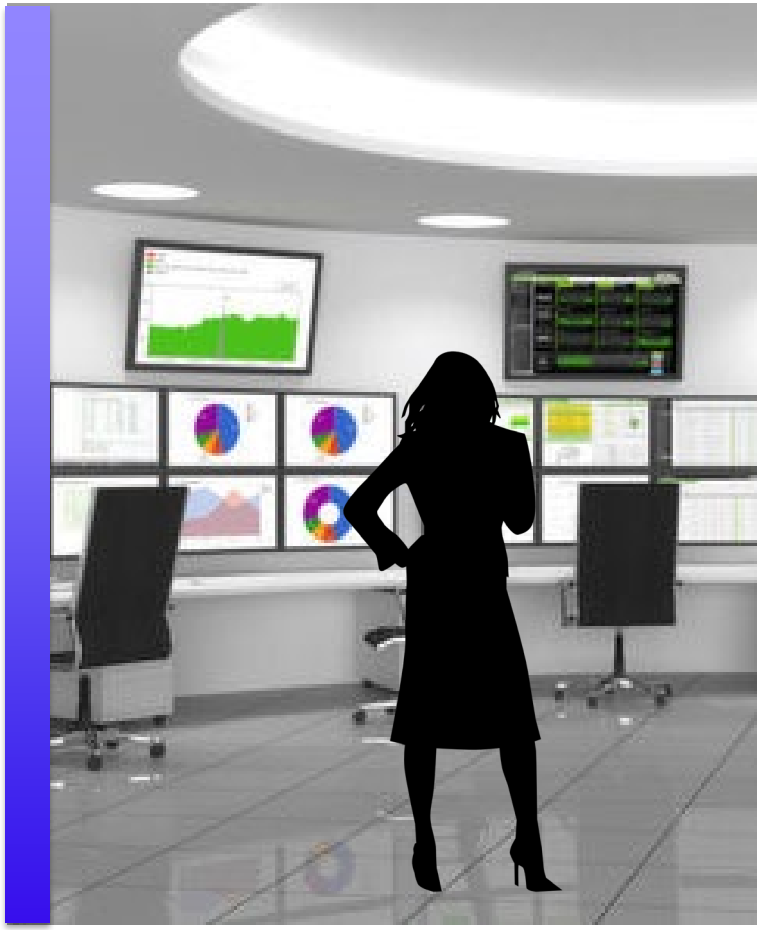
🔍 **Analysis:**

- The "True" First Line
- Operational ≠ First Line; Detection ≠ Prevention
- Assurance Role

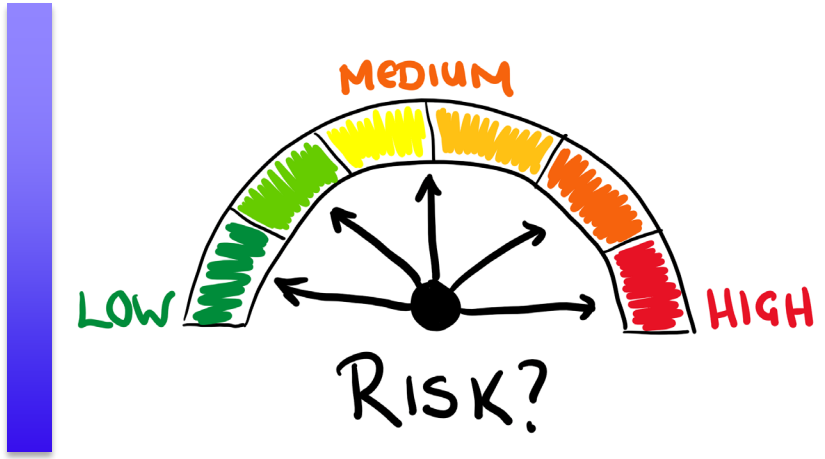
⚖️ **Verdict:** 🚨 **BUSTED!**

🛠️ **Takeaway: Rethink the SOC's function**

- Treat your SOC as an assurance function, not just a technical operation
- Ensure clear separation of duties
- Empower the "True" first line



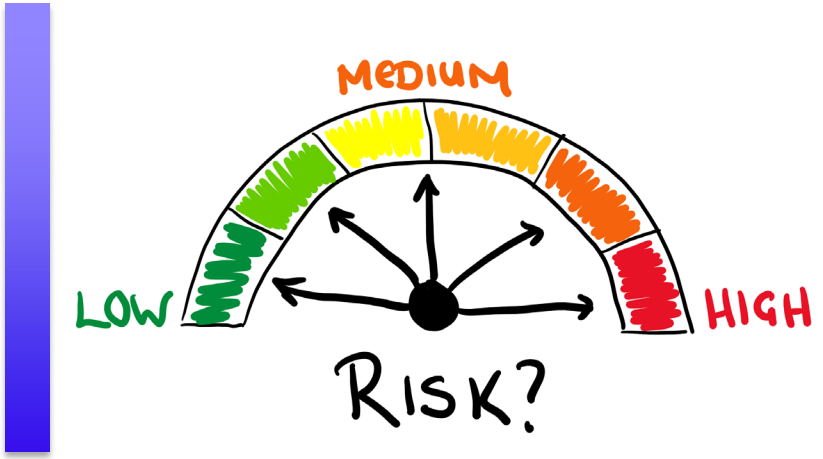
Myth 2: The board doesn't need to understand cyber security—That's the CISO's job.



Myth 2: The board doesn't need to understand cyber security—That's the CISO's job.

🔍 **Analysis:**

- Oversight vs Management
- Differentiate cybersecurity and cyber risk
- e.g., CFOs **translate** financials; CISOs **translate** cyber
- Regulation & accountability is **increasing**



Myth 2: The board doesn't need to understand cyber security—That's the CISO's job.

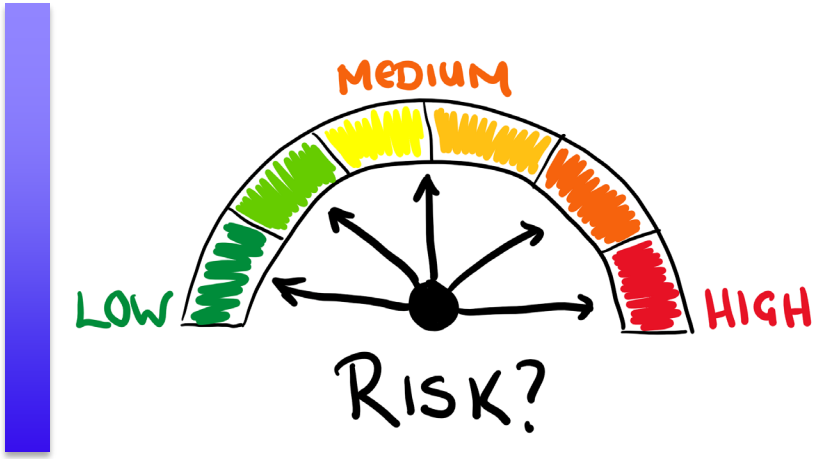
🔍 **Analysis:**

- Oversight vs Management
- Differentiate cybersecurity and cyber risk
- e.g., CFOs **translate** financials; CISOs **translate** cyber
- Regulation & accountability is **increasing**

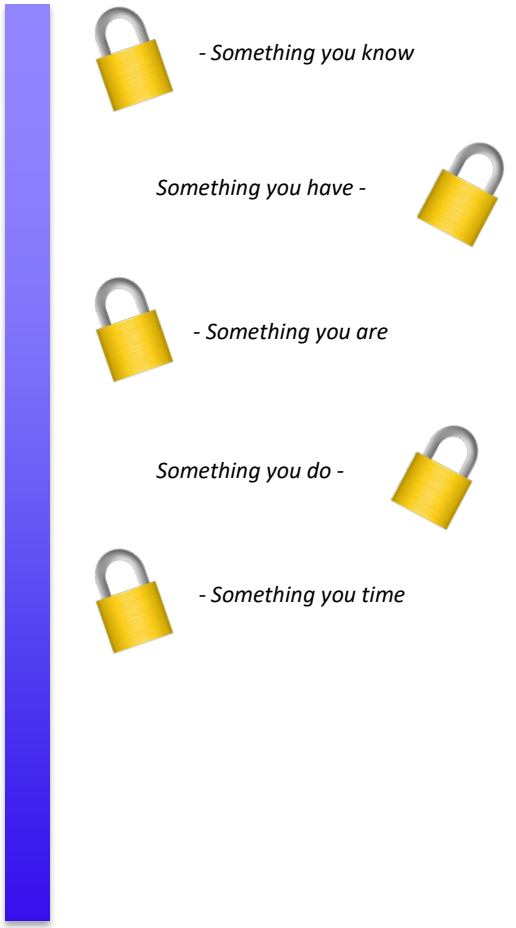
⚖️ **Verdict:** ✅ CONFIRMED**!**

🛠️ **Takeaways:**

- **Cyber = Business Risk**
- **Board Accountability**
- Basic cyber literacy is a must
- **CISO's Role** – Educate, not just inform



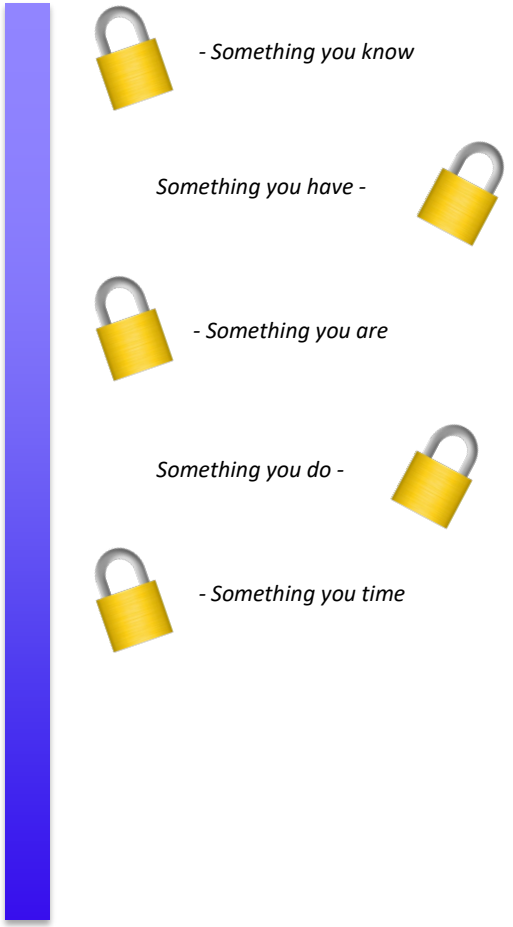
Myth 3: MFA is the strongest technical control.



Myth 3: MFA is the strongest technical control.

🔍 **Analysis:**

- **Proof** – actionable, intelligible, and cost-effective
- **Identity** is the new perimeter
- What's the **alternative**?



Myth 3: MFA is the strongest technical control.

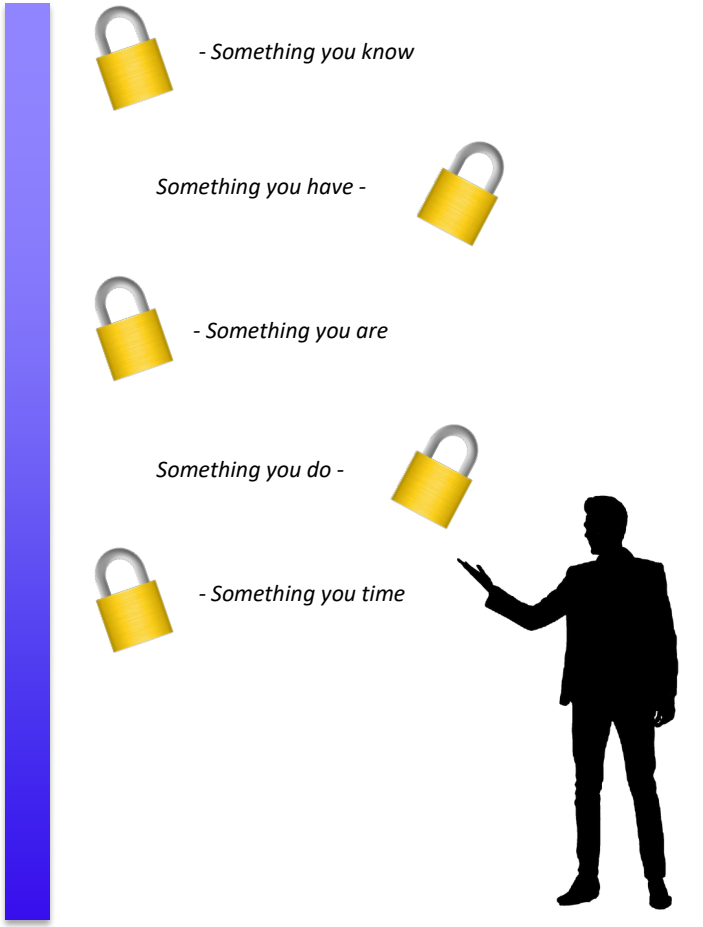
🔍 **Analysis:**

- **Proof** – actionable, intelligible, and cost-effective
- **Identity** is the new perimeter
- What's the **alternative**?

⚖️ **Verdict:** ⚠️ **PLAUSIBLE!**

🛠️ **Takeaway: Strengthen MFA's prerequisites**

- Assess coverage and defense-in-depth
- MFA is challenged by state-level law enforcement
- Hardware Keys are still great (at 5x factors)
- Where is your MFA Authenticator app hosted??



Myth 4: Cyber threats present the greatest risk to your company.

Myth 4: Cyber threats present the greatest risk to your company.

🔍 **Analysis:**

- Cyber risk is significant, but **context matters**
- **Risk** is threat-, industry-, and scenario-dependent
- **Maturity** matters
- Business-centric risk **appetite**

Myth 4: Cyber threats present the greatest risk to your company.

🔍 **Analysis:**

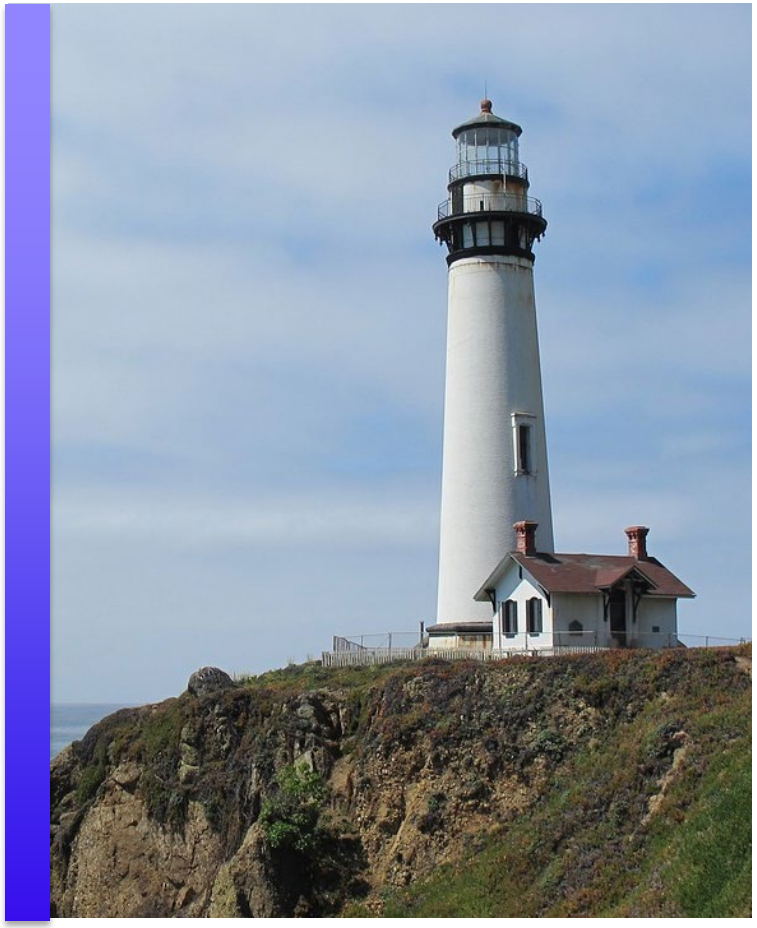
- Cyber risk is significant, but **context matters**
- **Risk** is threat-, industry-, and scenario-dependent
- **Maturity** matters
- Business-centric risk **appetite**

⚖️ **Verdict:** ⚠️ **PLAUSIBLE!**

🛠️ **Takeaway: Prioritize Cyber in Context**

- Align cyber risk with top business risks
- Position cyber as a risk management function
- Recognize cyber risk may be vital, but not existential

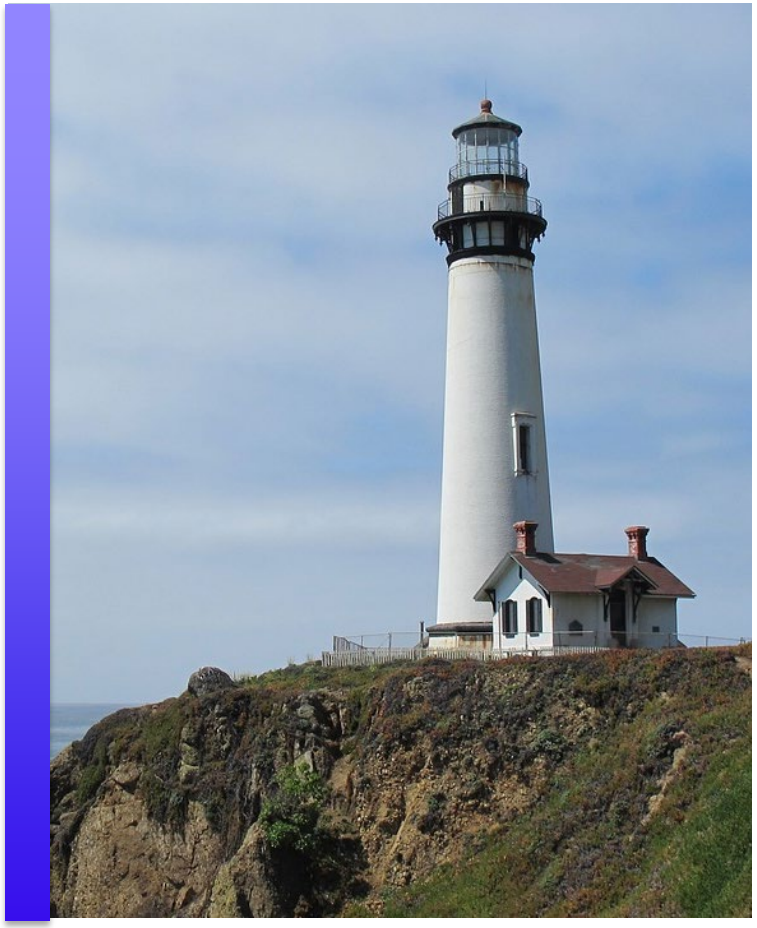
Myth 5: CISOs are business & culture leaders first, and technology leaders second.



Myth 5: CISOs are business & culture leaders first, and technology leaders second.

🔍 **Analysis:**

- Technology is Core
- Business & Risk Fluency = Influence
- Security Culture as a Value Driver
- Change Management



Myth 5: CISOs are business & culture leaders first, and technology leaders second.

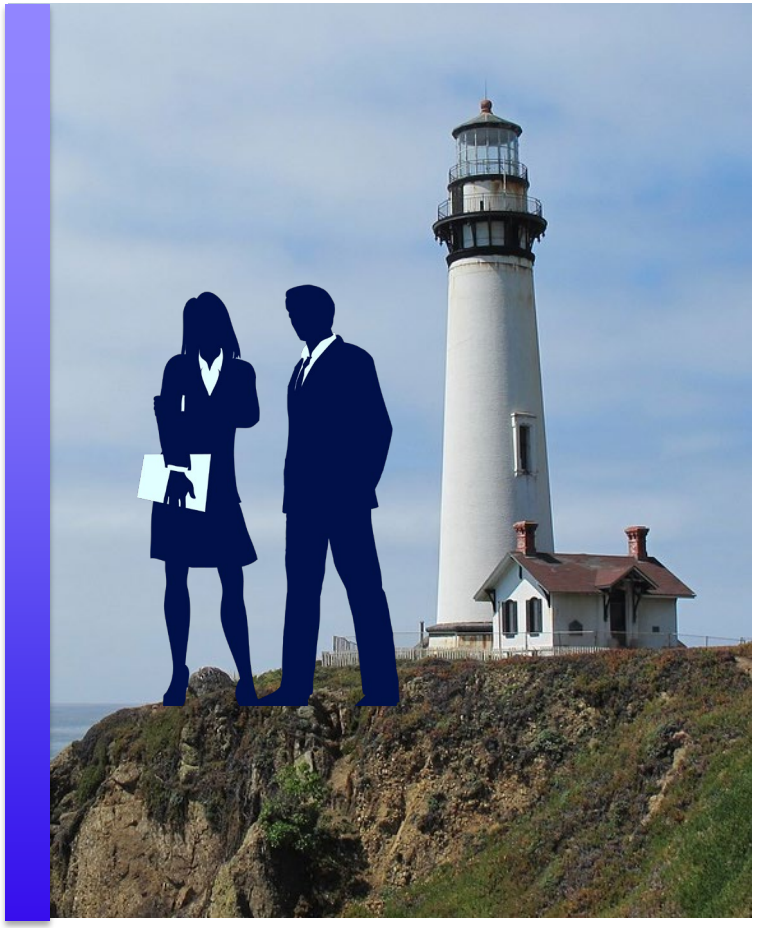
🔍 **Analysis:**

- Technology is Core
- Business & Risk Fluency = Influence
- Security Culture as a Value Driver
- Change Management

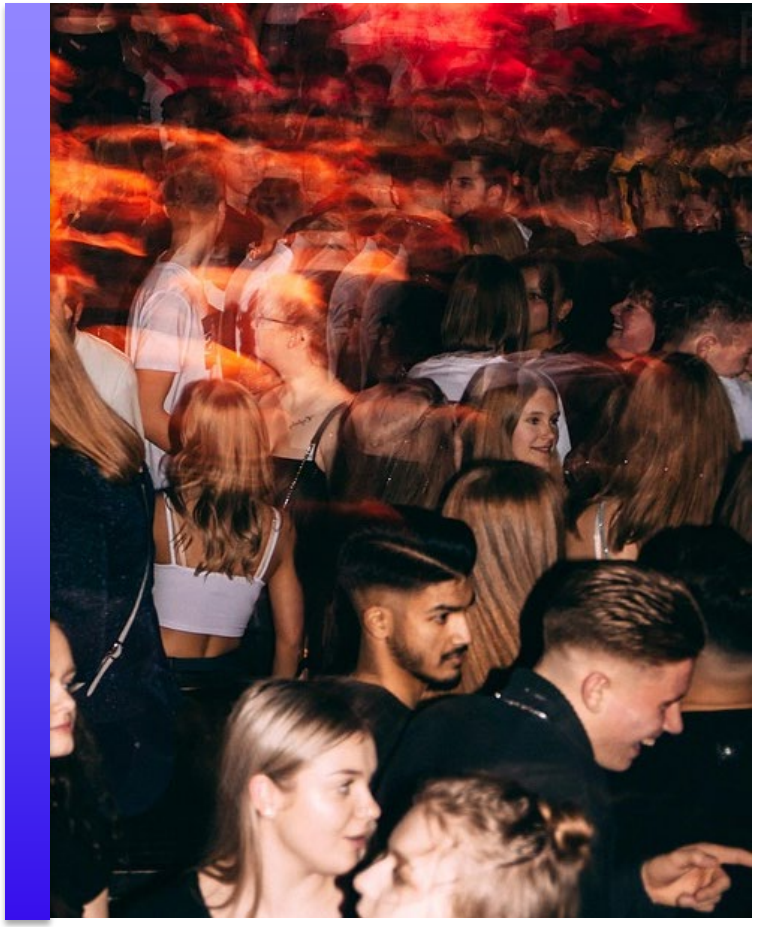
⚖️ **Verdict:** ✅ **CONFIRMED!**

🛠️ **Takeaway: Rethink the CISO Role**

- Develop financial and business acumen
- Translate security into ROI
- Align security metrics with business outcomes



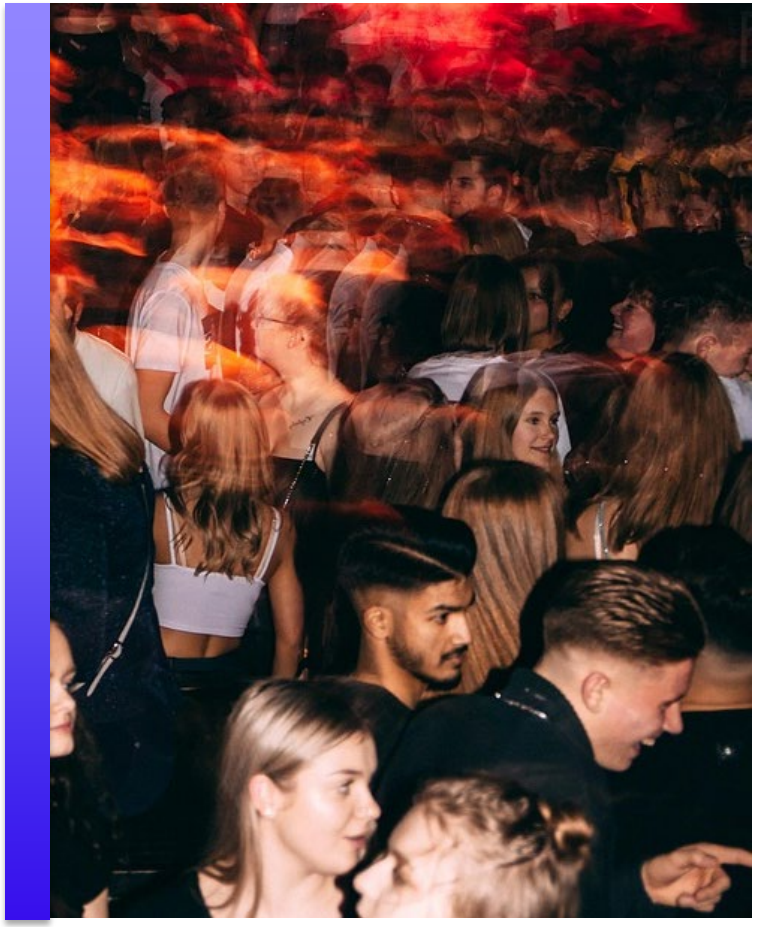
Myth 6: Third Party Risk Management is a wasted effort.



Myth 6: Third Party Risk Management is a wasted effort.

🔍 **Analysis:**

- Questionnaires and SOC 2s can be gamed
- Legal rarely enforces the contract
- Best-effort oversight is better than nothing
- Critical != high risk



Myth 6: Third Party Risk Management is a wasted effort.

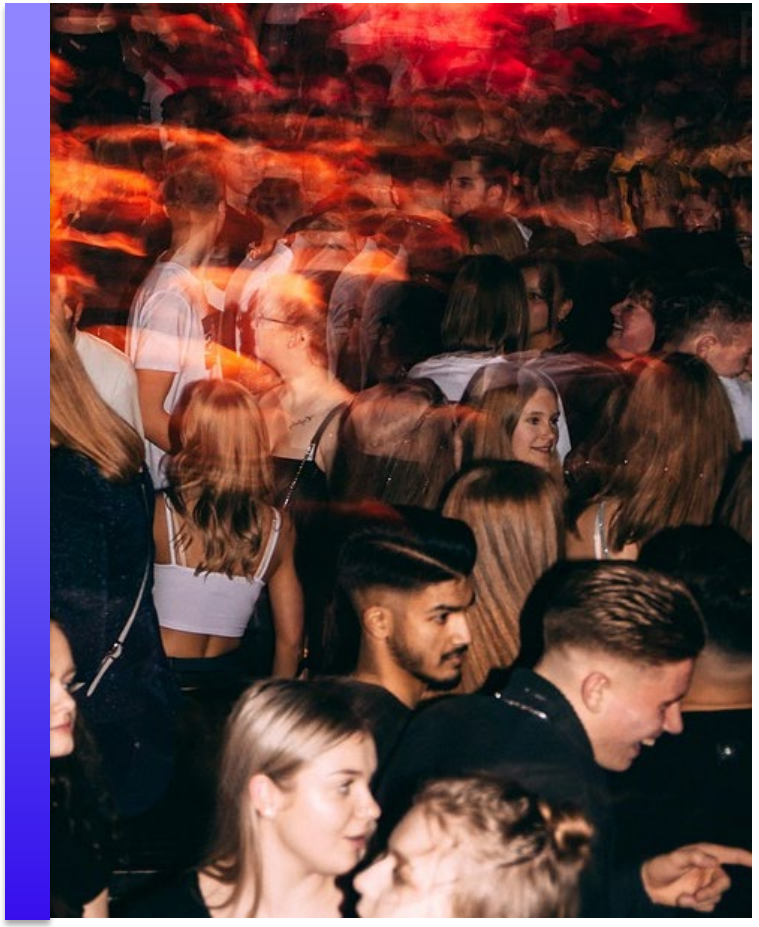
🔍 **Analysis:**

- Questionnaires and SOC 2s can be gamed
- Legal rarely enforces the contract
- Best-effort oversight is better than nothing
- Critical != high risk

⚖️ **Verdict:** ⚠️ **PLAUSIBLE!**

🛠️ **Takeaways: Move Beyond Paper Compliance**

- **Risk-Tier Vendors** – Focus on those that matter most
- **Monitor Continuously** – Risks evolve



Myth 7: Insurability is the new compliance.

Myth 7: Insurability is the new compliance.

🔍 **Analysis:**

- Insurability will soon **drive** compliance
- Insurance has **strategic** value
- Insurance **opens** the door; beware exclusions
- Payouts rarely cover the **full cost** of an incident

Myth 7: Insurability is the new compliance.

🔍 **Analysis:**

- Insurability will soon **drive** compliance
- Insurance has **strategic** value
- Insurance **opens** the door; beware exclusions
- Payouts rarely cover the **full cost** of an incident

⚖️ **Verdict:** ⚠️ **PLAUSIBLE!**

🛠️ **Takeaway:** Understand your policy

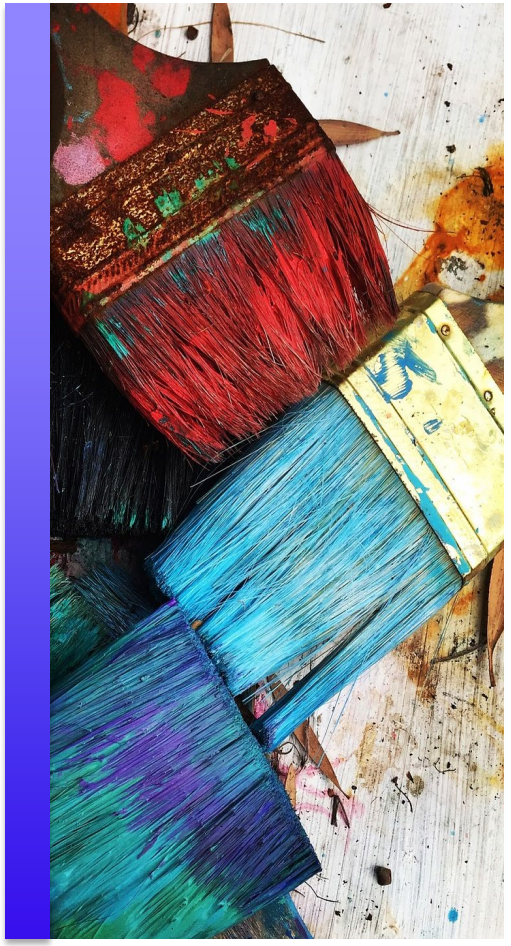
- Meet (or exceed) security requirements
- Be ready for Claim challenges
- Insurance is a safety net, **not** an operational strategy

Apply what you have learned today

✅ **Next Week:**
- Identify 1-2 **myths** in your organization, and start conversations
- Review your **SOC, TPRM, or cyber insurance policies**—gaps?
- Challenge a compliance requirement—does it actually improve security?

✅ **In Three Months:**
- Map **compliance vs. security gaps** in your program
- Strengthen **vendor accountability** with real security requirements
- Improve **incident readiness**

✅ **In Six Months:**
- Shift security from **checkbox-driven** to **risk-driven** strategies
- Align **business and security teams**—bridge the gap in expectations
- Create a **myth-busting mindset**—deliver real change



RSAC 2025 Conference

Many Voices.
One Community.

Security evolves. So should your approach. 🔥 Let's get to work.

Thank you!

For more information contact

Scott Brammer or Dan Gorecki